

Key rate enhancement using qutrit states for uncharacterized quantum key distribution

Yonggi Jo¹ and Wonmin Son^{1,2}

¹*Department of Physics, Sogang University, 35, Baekbeom-ro, Mapo-gu, Seoul 04107, Republic of Korea*

²*Department of Physics, University of Oxford, Parks Road, Oxford OX13PU, United Kingdom*

It is known that measurement-device-independent quantum key distribution (MDI-QKD) provides ultimate security from all types of side-channel attack against detectors at the expense of low key generation rate. Here, we propose MDI-QKD using 3-dimensional quantum states and show that the protocol improves the secret key rate under the analysis of mismatched-basis statistics. Specifically, we analyze security of the 3d-MDI-QKD protocol with uncharacterized sources, meaning that the original sources contain unwanted states instead of expected one. We simulate secret key rate of the protocol and identify the regime where the key rate is higher than the protocol with the qubit MDI-QKD.

I. INTRODUCTION

Quantum cryptography is a matured application of quantum informational theory which exploits quantum mechanical principle. In its core, there is a process called quantum key distribution (QKD) [1, 2] generating secure key between two distant parties, Alice and Bob, against a possible eavesdropper called Eve. There were many researches for proving security of QKD based on quantum mechanical effects [3–7] and experiments for demonstrating QKD system [8–13].

It is notable that the early QKD protocols use two dimensional quantum state, called qubit [14]. Due to its extensible structure, it is expected that high dimensional quantum state is able to carry more information per single quanta compared with qubit. Till now, high dimensional quantum systems on photon were studied for quantum communication in a various context. There were theoretical ideas to exploit high dimensional quantum states in quantum information processing, for example, nonlocality test [15, 16], entanglement measurement [17] and quantum teleportation [18, 19]. Experimentally, high dimensional quantum states are demonstrated in various quantum systems, energy-time entangled states [20, 21], position and momentum entangled states [22, 23], multi path-entangled states [24], and orbital angular momentum(OAM) mode [25, 26]. High dimensional quantum states are applied in QKD protocol as well. There were researches for proving security of QKD using d -dimensional quantum system which is generalized version of original QKD protocol [27–32]. These results show that QKD using high dimensional quantum states has higher upper bound on the error rate that ensures unconditional security of the channel. QKD protocols using high dimensional quantum states are demonstrated by using time-energy states [33–36], spatial modes [37, 38], and OAM modes [39, 40], so far.

In the other side of QKD investigation, security of practical QKD system has also been scrutinized in detail. Many theoretical security proofs have been made under the assumptions that all devices are trusted or well characterized for perfect security. However, in a real

situation, it becomes necessary to inspect the case that untrusted devices are used seriously because they may be produced by eavesdropper or they just cannot be operated as expected. On the other hand, attack models which exploit imperfect devices, called side channel attack, are proposed and demonstrated recently. They were photon number splitting (PNS) attack [41], faked-state attack [42], detector efficiency mismatch attack [43], detector blinding attack [44], time-shift attack [45], and laser damage attack [46]. From the study of hacking QKD system, it is known that imperfection of devices in the system brings serious security problems. There are security patches for each of the attacks, for example using decoy states for preventing PNS attack [47], but we need to defend all attacks even including undiscovered one for ensuring perfect security of QKD.

In order to extend the notion of ultimate security, device-independent QKD (DI-QKD) protocol is proposed in 2007 [48, 49]. In the DI-QKD study, they proposed a secure QKD scheme that is independent of the device imperfection while the security is guaranteed by non-local correlation identified by Clauser-Horne-Shimony-Holt (CHSH) type inequality [50]. However, it has been turned out that DI-QKD is not easy to be implemented in practice because it requires high quality entanglement source, low-loss against noisy channel and highly efficient detectors. Compensating the practicality, measurement-device-independent QKD (MDI-QKD) protocol is proposed in 2012 [51]. In MDI-QKD scheme, all types of possible side channel attack exploiting imperfection of detectors are overcome by separating detectors from Alice and Bob. For the separation, potentially untrusted third party, called Charlie, is introduced for their QKD. Alice and Bob send their encoded photon to Charlie, then Charlie performs a special type of composite measurement on his incoming photon pair, called Bell state measurement (BSM). After the BSM, Charlie announces the measurement result to Alice and Bob through the classical channel, then the two party establish the correlation between their photon when their encoding bases are same. From the fact that Charlie only act as a referee for the correlation between Alice and Bob, he cannot

access to the encoded message as like eavesdropper and it guarantees the unbounded security between Alice and Bob.

Thus, by using MDI-QKD, we can overcome the most of side channel attacks when the major security issues are attributed to the imperfections of detectors [52]. The other advantage of MDI-QKD is that no entanglement is needed like BB84 protocol. There were several experiments to demonstrate MDI-QKD using different physical systems, *e.g.* with time-bin states [53] and polarization states [54]. Especially, the latter realized the long distance MDI-QKD over 200km [55].

In the mean while, the practical MDI-QKD still suffers from its low key rate compared with BB84 protocol together with high quality requirement that the communication source should satisfy. MDI-QKD needs BSM setup that has only 50% success probability using linear optical elements [56]. Such the success probability of BSM is mainly responsible for a low key generation rate of MDI-QKD.

In this work, we propose MDI-QKD protocol using 3-dimensional quantum state (3d-MDI-QKD) which allows the improvement of the secret key rate compared with the original protocol using qubits. In the security analysis, we focus on asymptotic key rates. We analyze the security of 3d-MDI-QKD under the assumption that the states generated from communication sources are not ideally prepared, which is called the uncharacterized sources assumption. We use the mismatched-basis statistics in security analysis for 3d-MDI-QKD with uncharacterized sources as it is proposed for qubit MDI-QKD in [57]. Here, we show that there is the improvement of the security in 3d-MDI-QKD compared with qubit MDI-QKD in theoretical model, even if the communication sources are uncharacterized. We simulate the secret key rate of 3d-MDI-QKD with the change of the realistic experimental factors and identify the regime where 3d-MDI-QKD is more secure than qubit MDI-QKD.

This article is organized as following. In section II, we present the schematic description of 3d-MDI-QKD. In section III, we analyze the security of 3d-MDI-QKD with uncharacterized sources by using the analysis of the mismatched-basis statistics. In section IV, we simulate the secret key rate of 3d-MDI-QKD and compare it with that of qubit MDI-QKD in the theoretical model and in the realistic experiment model. Finally, we conclude in section V. Details of calculation are given in the Appendix.

II. MDI-QKD USING 3-DIMENSIONAL QUANTUM STATES

In this section, we present the schematic description of 3d-MDI-QKD. As its extension of the original qubit MDI-QKD protocol [51], we assume that Alice and Bob use two measurements at each site. In the original protocol, they use two orthonormal states to encode classical

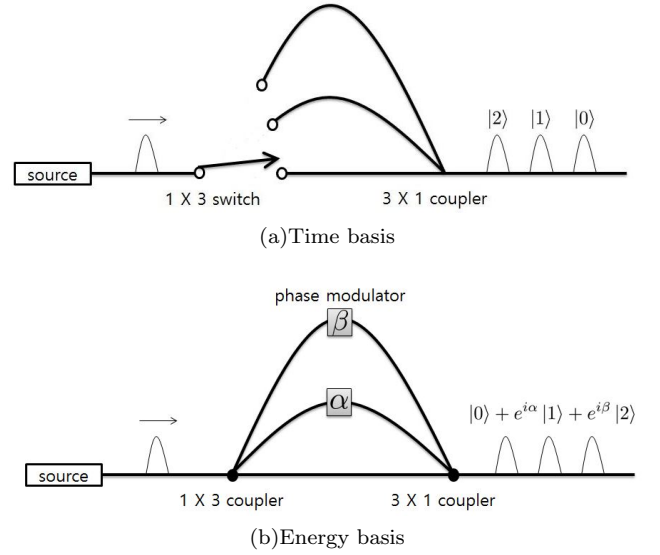


FIG. 1. A schematic setup to generate 3-dimensional quantum states of two bases[33]. In time basis (a), Alice and Bob encode information in time states of photon. In this setup, the time states are generated with three different delay lines and switch. The time that photon injected into the output port can be controlled with choice of delay line. $|0\rangle$, $|1\rangle$ and $|2\rangle$ denote time states when photon passes through the shortest, the middle, and the longest delay line respectively. In energy basis (b), Alice and Bob prepare similar settings with phase modulators on delay lines and 1×3 coupler instead of switch. From Eq. (1), in order to generate the states in the energy basis, $\{e^{i\alpha}, e^{i\beta}\}$ should be $\{1, 1\}$, $\{\omega^2, \omega\}$, and $\{\omega, \omega^2\}$ to generate $|\bar{0}\rangle$, $|\bar{1}\rangle$ and $|\bar{2}\rangle$ respectively.

binary bits 0 and 1. In our protocol, Alice and Bob use two measurements at each site whose bases for the measurement outcomes are consisted of three orthonormal states. We assume that the two different measurements are prepared in mutually unbiased bases (MUBs). The condition for two bases to be MUBs in 3-dimensional Hilbert space is that $|\langle i|\bar{j}\rangle|^2 = 1/3$ for all $i, j \in \{0, 1, 2\}$, where $\{|0\rangle, |1\rangle, |2\rangle\}$ and $\{|\bar{0}\rangle, |\bar{1}\rangle, |\bar{2}\rangle\}$ are two orthonormal bases.

The 3-dimensional quantum states can be realized through the various photonic degree of freedom in practice [33, 37, 38, 40]. Fig. 1 shows schematic setup to generate 3-dimensional quantum states using the different path length of the optical fiber. QKD protocol using the encoding system is originally proposed in [33]. In the time basis (Fig. 1 (a)), Alice controls the time that photon is injected into the output port of the settings. This task can be accomplished by using 1×3 optical switch and the three different delay lines. The arrival time of photon at output port can be controlled since the delay lines have different path length. In Fig. 1 (a), $|0\rangle$, $|1\rangle$ and $|2\rangle$ denote the three time states when photon passes through the shortest, the middle, and the longest delay line respectively. The time intervals among these three time states must be large enough compared with pulse

duration of source. In that case, these three states can be distinguished by using measurement of arrival time of photon. In order to create states belonging to the energy basis, Alice uses the setup shown in Fig. 1 (b). The length of each delay lines should be same with that of the time basis. There are phase modulators and 1×3 coupler instead of 1×3 switch. 1×3 coupler splits a beam of light into three output ports with same probabilities. In that case, the output state of this setup is described by $\frac{1}{\sqrt{3}}(|0\rangle + e^{i\alpha}|1\rangle + e^{i\beta}|2\rangle)$ where α and β are phase factors that Alice can control. Using the operation, three orthogonal states of the other MUB can be generated and they are described as

$$\begin{aligned} |\bar{0}\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle) \\ |\bar{1}\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + \omega^2|1\rangle + \omega|2\rangle) \\ |\bar{2}\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + \omega|1\rangle + \omega^2|2\rangle), \end{aligned} \quad (1)$$

where $\omega^3 = 1$, $\omega^2 + \omega + 1 = 0$ [58], and $|\bar{0}\rangle$, $|\bar{1}\rangle$ and $|\bar{2}\rangle$ denote the orthonormal states in the energy basis. Throughout this paper, we denote two MUBs for $3d$ -MDI-QKD ordinary basis and bar basis. In the example, the ordinary basis and the bar basis are corresponding to the time basis and the energy basis respectively.

Before introducing $3d$ -MDI-QKD, it is necessary to redefine the representation of Bell state measurement (BSM) as to describe the maximally entangled states of 3-dimensional bipartite system. There are nine maximally entangled states in 3-dimensional bipartite system. We define $\{|\Phi_i\rangle\}$ as a set of 3-dimensional maximally entangled states where $i \in \{0, 1, \dots, 8\}$, and each state is described as

$$|\Phi_{3k+l}\rangle = \frac{1}{\sqrt{3}} \sum_{m=0}^2 \omega^{ml} |m+k, m\rangle \quad (2)$$

where $k, l \in \{0, 1, 2\}$. We omit (mod 3) from all indices as a matter of simplification. Then the 3-dimensional BSM ($3d$ -BSM) is defined as a set of projections $\{\hat{B}_i|\hat{B}_i = |\Phi_i\rangle\langle\Phi_i|\}$.

From now on, we discuss the procedure of $3d$ -MDI-QKD. Similarly like the original protocol [51], Alice (Bob) firstly chooses an integer number, indexed i , among 0, 1, 2, $\bar{0}$, $\bar{1}$, and $\bar{2}$ randomly. Then she (he) generates the corresponding state $|i\rangle$ and sends it to untrusted third party called Charlie. With the states, Charlie performs $3d$ -BSM on the incoming photons and announces the result of measurement through the public channel. After the measurement, Alice and Bob share the information about the encoding basis through the public channel. Subsequently, after the basis comparison, they discard the trial if the original bases are different. The remaining data becomes sifted key after post-process based on the result of $3d$ -BSM. In order to synchronize the encoded information, it is necessary to perform the appropriate

post-process. The method of post-process is described in Table I.

To evaluate the usefulness of the protocol, it is necessary to analyze security of $3d$ -MDI-QKD. The analysis can be made through the detailed inspection of the equivalent protocol using entanglement distillation process (EDP) [3, 5, 6]. The idea is that if Alice and Bob share the maximally entangled state, Eve can not generate correlation between her state and the state of Alice and Bob [59]. The property of entanglement is called monogamy of entanglement. In the sense, QKD is always secure when Alice and Bob share the maximally entangled states. Therefore, in this case, we can analyze security of $3d$ -MDI-QKD with the amount of maximally entangled states between Alice and Bob generated from EDP. The equivalent protocol that exploit the entangled pair can be found as follows.

1. Alice and Bob prepare photon pair in a maximally entangled state $|\Phi_0\rangle$. Labels of Alice's photons are denoted as A and C, and those of Bob's photons are B and D. In the situation, they start with the pairs of entanglement as
- $$|\Phi_0\rangle_{AC} = \frac{1}{\sqrt{3}}(|0, 0\rangle_{AC} + |1, 1\rangle_{AC} + |2, 2\rangle_{AC}) \quad (3)$$
- $$|\Phi_0\rangle_{BD} = \frac{1}{\sqrt{3}}(|0, 0\rangle_{BD} + |1, 1\rangle_{BD} + |2, 2\rangle_{BD}).$$
2. Alice (Bob) sends photon C (D) to Charlie.
 3. Charlie performs $3d$ -BSM onto the incoming photons, and announces his result of measurement to Alice and Bob.
 4. The photon A and B become one of maximally entangled state after $3d$ -BSM [60] if there is no loss and there is no Eve.

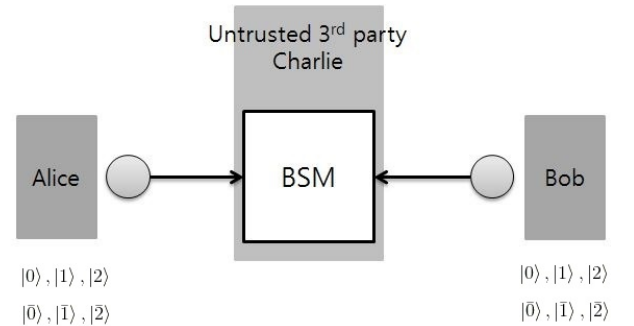


FIG. 2. A schematic diagram of MDI-QKD using 3-dimensional quantum states ($3d$ -MDI-QKD). BSM means Bell-state measurement. In 3-dim MDI-QKD, BSM should be able to discriminate 3-dimensional maximally entangled states.

BSM result Basis	$ \Phi_0\rangle$	$ \Phi_1\rangle$	$ \Phi_2\rangle$	$ \Phi_3\rangle$	$ \Phi_4\rangle$	$ \Phi_5\rangle$	$ \Phi_6\rangle$	$ \Phi_7\rangle$	$ \Phi_8\rangle$
Ordinary basis	-	-	-	$l \rightarrow$ $l+1$	$l \rightarrow$ $l+1$	$l \rightarrow$ $l+1$	$l \rightarrow$ $l+2$	$l \rightarrow$ $l+2$	$l \rightarrow$ $l+2$
Bar basis	$1 \leftrightarrow 2$	$0 \leftrightarrow 2$	$0 \leftrightarrow 1$	$1 \leftrightarrow 2$	$0 \leftrightarrow 2$	$0 \leftrightarrow 1$	$1 \leftrightarrow 2$	$0 \leftrightarrow 2$	$0 \leftrightarrow 1$

TABLE I. In 3d-MDI-QKD protocol, Alice and Bob communicate with each other in order to share the information about the encoding basis. After that, they should do post-process based on result of 3d-BSM in order to generate sifted key. In the Table, we represent the post-process method for the case that Alice preserves hers data, and Bob modifies his data. (mod 3) is omitted from the indices and $l \in \{0, 1, 2\}$.

5. In order to obtain $|\Phi_0\rangle_{AB}$, Bob does unitary operation on his photon based on the result of 3d-BSM.
6. Alice (Bob) chooses measurement basis and measures hers (his) photon A (B).
7. Alice and Bob compare their measurement bases and accept the encoded number as a key only when they have used the same measurement bases.
8. If Alice and Bob used bar bases, Bob do post-process to synchronize information. (See Table I)
9. The remaining data is used as sifted key.

In step 5, Alice and Bob share the maximally entangled state $|\Phi_0\rangle_{AB}$ if there is no error and no Eve. Then this entanglement version of 3d-MDI-QKD becomes same with 3-dimensional case of d -dimensional entanglement based protocol proposed in [29]. Security analysis of the d -dimensional entanglement based protocol has been studied in the previous works, against individual attack [29] (Eve monitors states separately) and against collective attack [30, 31] (Eve monitors several states jointly). According to the results, the secret key rate of 3d-MDI-QKD per sifted key against collective attack is evaluated as

$$r \geq \log_2 3 - 2Q - 2H(Q) \quad (4)$$

where $H(x)$ is Shannon entropy defined as $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ and Q denotes state error rate in the ordinary basis. If the state that Alice and Bob share at the end of protocol is not $|\Phi_i\rangle$ where $i = 0, 1, 2$ then the trial has the state error in the ordinary basis. Then the state error rate in the ordinary basis is described by

$$Q = \sum_{i \neq j} \langle i, j | \hat{\rho} | i, j \rangle, \quad (5)$$

where $\hat{\rho}$ is density operator of Alice and Bob, and $i, j \in \{0, 1, 2\}$. In the ideal case without eavesdropper, the state is remained to be $\hat{\rho} = |\Phi_0\rangle \langle \Phi_0|$, so thus the error rate becomes trivial since $Q = 0$.

III. 3d-MDI-QKD WITH UNCHARACTERIZED SOURCES

MDI-QKD has an advantage that prevents all type of side channel attack against detectors. It also guar-

antees the security even if detectors are fabricated or controlled by Eve. In order to ensure the perfect security of MDI-QKD, there must be the assumption that sources used in QKD are ideally prepared without error. The states generated from the sources are well characterized in the assumption. For example, sources should generate one of the states among $\{|H\rangle, |V\rangle, |+\rangle, |-\rangle\}$ in the original MDI-QKD to guarantee the perfect security. Here $|H\rangle$ is a single photon state with horizontal polarization, $|V\rangle$ is a photon with vertical polarization, and $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$. However, in real QKD setup, communication sources can have misalignment in their encoding system and the states generated from the communication sources can be prepared differently from the wanted state.

Through the analysis of mismatched-basis statistics (MBS), it is proven that QKD with uncharacterized sources can also be secure against possible channel eavesdropping [57]. In the original QKD protocol, the data

(a) Ideal case										
BSM \ x, y	0,0	0,1	0,2	1,0	1,1	1,2	2,0	2,1	2,2	
$p(x, y)$	1/3	0	0	0	1/3	0	0	0	1/3	
BSM \ x, y	0, $\bar{0}$	0, $\bar{1}$	0, $\bar{2}$	1, $\bar{0}$	1, $\bar{1}$	1, $\bar{2}$	2, $\bar{0}$	2, $\bar{1}$	2, $\bar{2}$	
$p(x, y)$	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	

(b) Misalignment case										
BSM \ x, y	0, $\bar{\beta}_0$			1, $\bar{\beta}_0$			2, $\bar{\beta}_0$			
$p(x, y)$	$(\cos^2 \mu \sin^2 \nu)/3$			$(\sin^2 \mu \sin^2 \nu)/3$			$(\cos^2 \nu)/3$			

TABLE II. The success probabilities of 3d-BSM $p(x, y)$ when Alice and Bob send $|x\rangle$ and $|y\rangle$ to Charlie. We assume that 3d-BSM is able to discriminate only $|\Phi_0\rangle$ and there is no loss and no Eve. The success probabilities of 3d-BSM are calculated from $\text{Tr}[\hat{\rho}_{AB} |\Phi_0\rangle \langle \Phi_0|]$. (a) In ideal case, Alice and Bob send the state in the ordinary basis or the bar basis. Since these two bases are MUBs, the success probabilities of mismatched-basis cases are same with 1/9. (b) In misalignment case, we assume that Bob's encoder has misalignment while Alice's is perfect. Bob's source generates $|\bar{\beta}_0\rangle$ instead of $|\bar{0}\rangle$, where $|\bar{\beta}_0\rangle = \cos \mu \sin \nu |0\rangle + \sin \mu \sin \nu |1\rangle + \cos \nu |2\rangle$ for arbitrary angle μ and ν . The success probabilities of mismatched-basis cases are modified from 1/9.

that is obtained from the mismatched-basis are discarded because Alice and Bob cannot extract any information from it. However, in [57], they argue that the misalignment of communication sources influence to the MBS such that Alice and Bob can still extract secret key partially with the analysis of MBS even if the sources are uncharacterized.

Table II shows that the effect of misalignment in the prepared states modifies the MBS in 3d-MDI-QKD. At first, we consider the security for the case that 3d-BSM produces one of the maximally entangled state, *e.g.* $|\Phi_0\rangle$. In general, the number of possible entangled states that is generated from BSM affects to the sifted key rate. Due to the straightforward relationship, the security proof under the shared single Bell state can be easily generalized to the ideal BSM setup which is able to distinguish all of the nine maximally entangled states.

In the Table, $p(x, y)$ denotes success probability of 3d-BSM under the assumption of discriminating single Bell state after Alice and Bob send the states $|x\rangle$ and $|y\rangle$ to Charlie respectively. Table II (a) shows the probabilities when the communication sources for the sender's states are prepared perfectly. In Table II (b), we assume that Bob's source has misalignment while Alice's is perfect. Bob's source generates $|\bar{\beta}_0\rangle$ instead of $|\bar{0}\rangle$. The misaligned state $|\bar{\beta}\rangle$ is defined as $|\bar{\beta}_0\rangle = \cos \mu \sin \nu |0\rangle + \sin \mu \sin \nu |1\rangle + \cos \nu |2\rangle$ where μ and ν are arbitrary angles. It can be seen that all the probabilities of mismatched-basis case are 1/9 as in Table II (a). In comparison, the distribution of the success probabilities are changed when the basis is misaligned as shown in Table II (b). The change allows Alice and Bob to identify the accuracy of communication sources through the analysis of the MBS.

Before we analyze the security, we defined the explicit form of generated states from uncharacterized sources in detail. The states in the ordinary basis are $|\alpha_0\rangle$, $|\alpha_1\rangle$, and $|\alpha_2\rangle$ for Alice, $|\beta_0\rangle$, $|\beta_1\rangle$, and $|\beta_2\rangle$ for Bob. Subsequently, the states in the bar basis are $|\bar{\alpha}_0\rangle$, $|\bar{\alpha}_1\rangle$, and $|\bar{\alpha}_2\rangle$ for Alice and $|\bar{\beta}_0\rangle$, $|\bar{\beta}_1\rangle$, and $|\bar{\beta}_2\rangle$ for Bob. The relations between two bases are described as

$$\begin{aligned} |\bar{\alpha}_k\rangle &= \sum_{j=0}^2 A_{kj} e^{i\theta_{kj}} |\alpha_j\rangle \\ |\bar{\beta}_k\rangle &= \sum_{j=0}^2 B_{kj} e^{i\varphi_{kj}} |\beta_j\rangle, \end{aligned} \quad (6)$$

where A , B are non-negative real numbers and θ , φ are arbitrary phases. Since Alice and Bob cannot specify the details of generated states, we consider all the possible values of A , B , θ and φ for our security analysis. The 3-dimensional maximally entangled states are redefined to have arbitrary phases in the generated states. 3-dimensional maximally entangled states with the un-

determined phase factors are defined as

$$|\tilde{\Phi}_{3k+l}\rangle = \frac{1}{\sqrt{3}} \sum_{m=0}^2 \omega^{ml} e^{i(\delta_{m+k} + \xi_k)} |m+k, m\rangle, \quad (7)$$

where δ and ξ are phase factors stemmed from experimental setting, and it can be set $\delta_0 = \xi_0 = 0$.

The secret key rate obtained in Eq. (4) is to be modified for the case of uncharacterized communication source. In the ordinary basis, there are two different types of error Q_s and Q_p . Q_s is the state error rate explained in section II and Q_p is phase error rate which indicates the state error due to the phase factor. If Alice and Bob share the maximally entangled state with additional phase factor ω , for example $|\Phi_1\rangle$, then, Alice and Bob identify that there is phase error as it differ from $|\Phi_0\rangle$ up to the phase factor in the state. The phase error is comparable with the state error that exists in the bar basis.

Eq. (4) is obtained under the scenario of symmetric attack which is Eve's optimal attack against ideal QKD scheme. The symmetric attack is the strategy to extract the information from the two MUB measurements at both sides equally well [27, 29, 31]. Since this attack disturbs the measurement statistics equally for the two different measurement bases, the equivalence of two error rate $Q_s = Q_p$ can be observed. At the same time, these two errors should be discriminated to analyze the security for QKD with uncharacterized sources. If we split the effect of these two error rates, the secret key rate becomes

$$r \geq \log_2 3 - (Q_s + Q_p) - H(Q_s) - H(Q_p). \quad (8)$$

So if Alice and Bob calculate Q_s and Q_p , they can evaluate the secret key rate of 3d-MDI-QKD with uncharacterized sources.

We analyze the security with uncharacterized sources from the number of generated maximally entangled states using EDP. In the equivalent protocol with uncharacterized sources, Alice and Bob choose measurement basis before generating photon pair. According to their basis choices, they generate the different photon pairs. Alice (Bob) generates $|\psi\rangle_{AC}$ ($|\phi\rangle_{BD}$) if she (he) chooses ordinary basis, and $|\bar{\psi}\rangle_{AC}$ ($|\bar{\phi}\rangle_{BD}$) if not. These state are described as

$$\begin{aligned} |\psi\rangle_{AC} &= \frac{1}{\sqrt{3}} (|0, \alpha_0\rangle_{AC} + |1, \alpha_1\rangle_{AC} + |2, \alpha_2\rangle_{AC}) \\ |\bar{\psi}\rangle_{AC} &= \frac{1}{\sqrt{3}} (|\bar{0}, \bar{\alpha}_0\rangle_{AC} + |\bar{1}, \bar{\alpha}_1\rangle_{AC} + |\bar{2}, \bar{\alpha}_2\rangle_{AC}) \\ |\phi\rangle_{BD} &= \frac{1}{\sqrt{3}} (|0, \beta_0\rangle_{BD} + |1, \beta_1\rangle_{BD} + |2, \beta_2\rangle_{BD}) \\ |\bar{\phi}\rangle_{BD} &= \frac{1}{\sqrt{3}} (|\bar{0}, \bar{\beta}_0\rangle_{BD} + |\bar{1}, \bar{\beta}_1\rangle_{BD} + |\bar{2}, \bar{\beta}_2\rangle_{BD}). \end{aligned} \quad (9)$$

Using the entangled states, Alice and Bob proceed 3d-MDI-QKD protocol. After several repetition of the procedure, Alice and Bob get statistics of success probabilities of 3d-BSM as it is described in Table II. The statistics can be used for the security analysis of our protocol.

For the security analysis, we consider the state after the Eve's general attack that can be described as

$$\begin{aligned} & \hat{U}_E |\alpha_x\rangle_C |\beta_y\rangle_D |e\rangle_{Ea} |1\rangle_Z \\ &= \sqrt{(1-p(x,y))} |\Xi xy\rangle_E |0\rangle_Z + \sqrt{p(x,y)} |\Gamma xy\rangle_E |1\rangle_Z \end{aligned} \quad (10)$$

where \hat{U}_E is Eve's unitary operation. $|e\rangle_{Ea}$ is Eve's ancillary system and Z denotes the state for the Charlie's message. $|0\rangle_Z$ indicates when the BSM fail and $|1\rangle_Z$ does BSM succeed. $p(x,y)$ is success probability of 3d-BSM when Alice sends $|\alpha_x\rangle$ and Bob sends $|\beta_y\rangle$ to Charlie. $|\Xi xy\rangle_E$ is Eve's final state after eavesdropping when BSM fail, while $|\Gamma xy\rangle_E$ is Eve's final state after eavesdropping when BSM succeed. Eve's final state can be expressed as $|\Gamma xy\rangle_E = \sum_n \gamma_{xy}(n) |n\rangle_E$ where $\{|n\rangle\}$ is orthonormal basis of Eve's state. In this expression, $\gamma_{xy}(n)$ is complex number which is obtained from $\gamma_{xy}(n) = \langle n | \Gamma xy \rangle$. $\gamma_{xy}(n)$ satisfies $\sum_n |\gamma_{xy}(n)|^2 = 1$. In these expressions, we meant $x, y \in \{0, 1, 2, \bar{0}, \bar{1}, \bar{2}\}$. If we post-select only the case $|1\rangle_Z$ when 3d-BSM succeed, the state of Alice, Bob, and Eve in the ordinary basis is described as

$$\hat{\rho}_{ABE} = C \times P \left\{ \sum_{x,y=0} \sqrt{p(x,y)} |x, y, \Gamma xy\rangle_{ABE} \right\} \quad (11)$$

where we use the notation for projector as $P\{|x\rangle\} = |x\rangle\langle x|$ and C is for the normalization constant. The density operator of Alice and Bob is obtained when Eve's system is traced out.

$$\begin{aligned} \hat{\rho}_{AB} &= \text{Tr}_E [\hat{\rho}_{ABE}] \\ &= \frac{\sum_n P \left\{ \sum_{x,y=0}^2 \sqrt{p(x,y)} \gamma_{xy}(n) |x, y\rangle_{AB} \right\}}{\sum_{x,y=0}^2 p(x,y)}. \end{aligned} \quad (12)$$

The security proof under the eavesdropping scenario is achieved if Alice and Bob can get Q_s and Q_p . If they get these error rates, they can analyze security of their QKD system from Eq. (8). The state error rate Q_s is easily

obtained from Eq. (12) and Eq. (5). It becomes

$$Q_s = \frac{p(0,1) + p(0,2) + p(1,0) + p(1,2) + p(2,0) + p(2,1)}{\sum_{x,y=0}^2 p(x,y)}. \quad (13)$$

From Eq. (13), Q_s is calculated from success probabilities of 3d-BSM. The phase error rate Q_p is obtained by

$$\begin{aligned} Q_p &= \langle \tilde{\Phi}_1 | \hat{\rho} | \tilde{\Phi}_1 \rangle + \langle \tilde{\Phi}_2 | \hat{\rho} | \tilde{\Phi}_2 \rangle + \langle \tilde{\Phi}_4 | \hat{\rho} | \tilde{\Phi}_4 \rangle \\ &\quad + \langle \tilde{\Phi}_5 | \hat{\rho} | \tilde{\Phi}_5 \rangle + \langle \tilde{\Phi}_7 | \hat{\rho} | \tilde{\Phi}_7 \rangle + \langle \tilde{\Phi}_8 | \hat{\rho} | \tilde{\Phi}_8 \rangle. \end{aligned}$$

As the last 4 terms are included in the state error rate, the equation is simplified by the inequality,

$$Q_p \leq \langle \tilde{\Phi}_1 | \hat{\rho} | \tilde{\Phi}_1 \rangle + \langle \tilde{\Phi}_2 | \hat{\rho} | \tilde{\Phi}_2 \rangle + Q_s. \quad (14)$$

$\langle \tilde{\Phi}_1 | \hat{\rho} | \tilde{\Phi}_1 \rangle$ and $\langle \tilde{\Phi}_2 | \hat{\rho} | \tilde{\Phi}_2 \rangle$ include phase factors δ and ξ which are defined in Eq. (7). In the circumstance, Alice and Bob do not know the details of the phase factors since the communication sources are uncharacterized. For the true upper bound, one should consider the largest values of $\langle \tilde{\Phi}_1 | \hat{\rho} | \tilde{\Phi}_1 \rangle$ and $\langle \tilde{\Phi}_2 | \hat{\rho} | \tilde{\Phi}_2 \rangle$. With the maximum, the new upper bound of phase error rate can be found as

$$Q_p \leq \frac{2 \sum_n \left| \sum_{k=0}^2 \sqrt{p(k,k)} e^{i\zeta_k} \gamma_{kk}(n) \right|^2}{\sum_{x,y=0}^2 p(x,y)} + Q_s \quad (15)$$

where ζ is the phase which makes the first term maximum. There are γ and ζ factors comes from Eve's states. Alice and Bob can not determine these factors. What Alice and Bob want to get is the upper bound of phase error rate which can be calculated from the success probabilities of 3d-BSM only. We formulate the new upper bound of phase error rate as

$$Q_p \leq \varepsilon + Q_s, \quad (16)$$

where ε is the factor calculated from the success probabilities that is obtained from Eq. (6) and Eq. (10). It is defined as

$$\varepsilon = \max_{A,B} [f_{01}(A,B), f_{20}(A,B)], \quad (17)$$

where max means finding maximum value for the coefficients A, B defined in Eq. (6). Details of the calculation is described in Appendix. The function f is defined as

$$f_{xy}(A,B) = \begin{cases} 1 - Q_s & \text{if } A_{xm} B_{ym} = 0, \quad \forall m \in \{0, 1, 2\} \\ \min[S_{xy}(0), S_{xy}(1), S_{xy}(2)] & \text{otherwise.} \end{cases} \quad (18)$$

$S_{xy}(m)$ is the upper bound function of the first term in Eq. (15) defined as

$$S_{xy}(m) = \frac{2}{3A_{xm}^2 B_{ym}^2 \sum_{i,j=0}^2 p(i,j)} \left\{ \sqrt{\left[\sqrt{p(\bar{x}, \bar{y})} + \sum_{i \neq j} A_{xi} B_{yj} \sqrt{p(i,j)} \right]^2} + 2 \prod_{k=1}^2 D_{xym}(k) + \sum_{k=1}^2 D_{xym}(k) \right\}^2, \quad (19)$$

where $D_{xym}(k)$ denotes the expression

$$D_{xym}(k) = |A_{xm} B_{ym} - A_{x(m+k)} B_{y(m+k)}| \sqrt{p(m+k, m+k)}.$$

The function f is formed to find the smallest value of $S_{xy}(m)$ for m in order to obtain the tight upper bound of the first term of Eq. (15). $S_{xy}(m)$ exists only when $A_{xm} B_{ym} \neq 0$, because of the factor $1/A_{xm} B_{ym}$. If $A_{xm} B_{ym} = 0$ for all $m \in \{0, 1, 2\}$, no upper bound function $S_{xy}(m)$ can be determined. In this case, Alice and Bob conclude that the states generated from the uncharacterized sources are not suitable for QKD. The function f has the form that the phase error rate becomes one in the case.

ε is defined to identify the relations between $|\bar{\alpha}_0\rangle$ and $|\bar{\beta}_1\rangle$ as well as $|\bar{\alpha}_2\rangle$ and $|\bar{\beta}_0\rangle$ in Eq. (17). The success probabilities of 3d-BSM for these states are $p(\bar{0}, \bar{1}) = 0$ and $p(\bar{2}, \bar{0}) = 0$ in the ideal 3d-MDI-QKD. If communication sources are ideal, ε is zero. Then the secret key rate of d -MDI-QKD with uncharacterized sources in Eq. (8) becomes same with the secret key rate of ideal 3d-MDI-QKD in Eq. (4). If the states generated from uncharacterized sources are not the ideal states, then the factor ε becomes non-zero. In the case, the maximization of ε is required in order to obtain the optimized secret key rate.

In order to find the maximum value of the factor ε , Alice and Bob need to consider the constraints about the coefficients A and B . The constraints are obtained from MBS under the Eve's attack, modeled in Eq. (10). In the case that Alice and Bob send the single photon states $|\bar{\alpha}_x\rangle$ and $|\bar{\beta}_y\rangle$ to Charlie respectively, the success probability of 3d-BSM can be obtained as

$$p(\bar{x}, \bar{y}) = |{}_Z \langle 1 |_E \langle \Gamma \bar{x} y | \hat{U}_E |\bar{\alpha}_x\rangle_A |\bar{\beta}_y\rangle_B|^2$$

and if we substitute $|\bar{\alpha}_x\rangle$ in Eq. (6), we have

$$p(\bar{x}, \bar{y}) = |{}_Z \langle 1 |_E \langle \Gamma \bar{x} y | \hat{U}_E \left[\sum_{i=0}^2 A_{xi} e^{\theta_{xi}} |\alpha_i\rangle_A \right] |\bar{\beta}_y\rangle_B|^2. \quad (20)$$

Since Alice and Bob cannot determine the parameters in the Eve's side, $|\Gamma xy\rangle_E$ and θ , they need to consider the largest and the smallest values of undetermined factors for the constraints. Then, the constraints for Alice's

coefficient can be obtained from Eq. (20),

$$\begin{aligned} & -2 \sum_{l=0}^2 \left[A_{jl} A_{j(l+1)} \sqrt{p(l, i) p(l+1, i)} \right] \\ & \leq p(\bar{j}, i) - \sum_{l=0}^2 A_{jl}^2 p(l, i) \leq \\ & 2 \sum_{l=0}^2 \left[A_{jl} A_{j(l+1)} \sqrt{p(l, i) p(l+1, i)} \right] \end{aligned} \quad (21)$$

where $i \in \{0, 1, 2\}$ and $j \in \{0, 2\}$. Similarly, the constraints for Bob's coefficient can be obtained from the success probability of 3d-BSM when Alice and Bob send $|\alpha_x\rangle$ and $|\bar{\beta}_y\rangle$ to Charlie respectively. The constraints for Bob's states are

$$\begin{aligned} & -2 \sum_{l=0}^2 \left[B_{kl} B_{k(l+1)} \sqrt{p(i, l) p(i, l+1)} \right] \\ & \leq p(i, \bar{k}) - \sum_{l=0}^2 B_{kl}^2 p(i, l) \leq \\ & 2 \sum_{l=0}^2 \left[B_{kl} B_{k(l+1)} \sqrt{p(i, l) p(i, l+1)} \right] \end{aligned} \quad (22)$$

where $i \in \{0, 1, 2\}$ and $k \in \{1, 0\}$. Now, Alice and Bob have six constraints at each side. Using the constraints, Alice and Bob are able to calculate the upper bound of phase error rate with Eq. (16). Finally the secret key rate of 3d-MDI-QKD with uncharacterized source can also be obtained from the success probabilities of 3d-BSM.

IV. SIMULATION

In this section, we present the results for the secret key rate simulation of 3d-MDI-QKD and 3d-MDI-QKD with uncharacterized sources. In the simulation, we consider the communication scenario that is realized by single photon source only. First of all, we discuss the ideal 3d-MDI-QKD with uncharacterized sources. Since there is no Eve and the devices are perfectly implemented, the statistics of success probabilities in 3d-BSM becomes same as it is shown in Table II (a). The state error rate

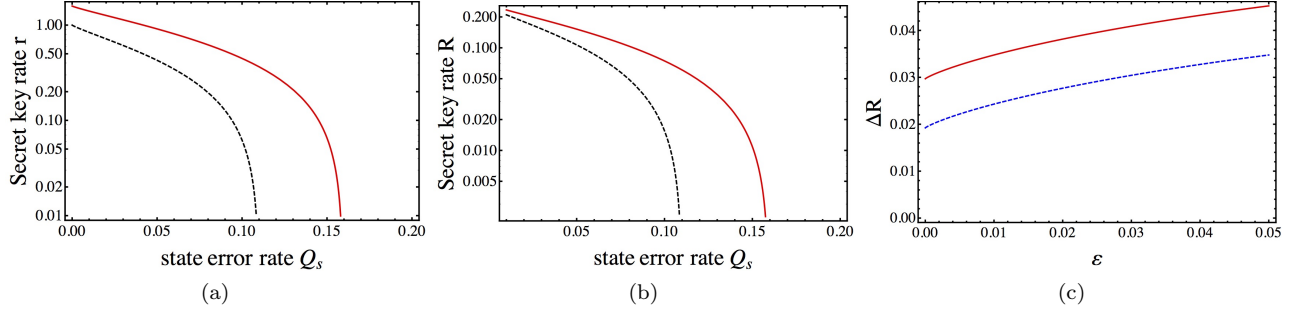


FIG. 3. (a) The secret key rate per sifted key r of original MDI-QKD (black, dashed line) and 3d-MDI-QKD (red line). (b) Secret key rate R per total signal of original qubit MDI-QKD (black, dashed line) and 3d-MDI-QKD (red line). We assumed 3d-BSM is able to discriminate three maximally entangled states among nine, and qubit BSM can discriminate two Bell states among four. (c) The difference between the secret key rate R of original MDI-QKD and 3d-MDI-QKD. Both secret key rates are obtained under the assumption of uncharacterized sources. ε is the factor which is defined in Eq. (16). Blue, dashed line shows difference between the secret key rates when the state error rate is fixed as $Q_s = 0.01$, red line shows the difference when $Q_s = 0.05$.

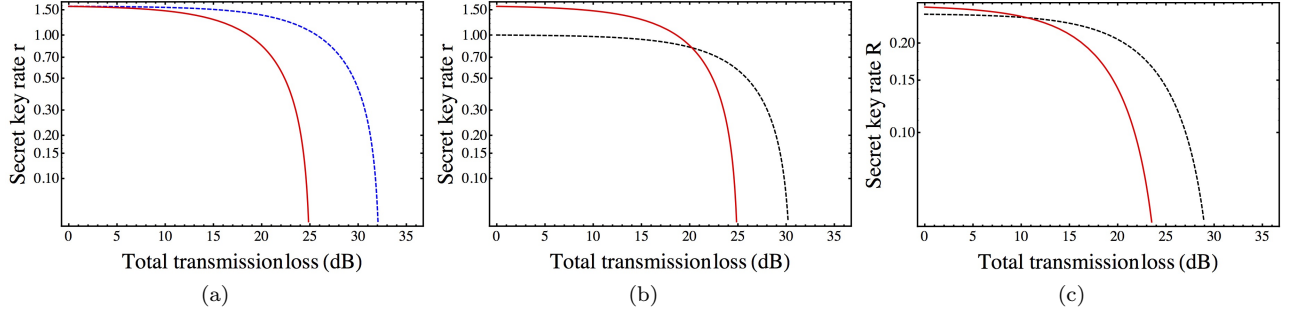


FIG. 4. The secret key rate of MDI-QKD vs. total transmission loss of optical channel. The dark count rate of single photon detector is assumed as 10^{-5} per pulse. We assume there is no Eve. (a) The secret key rate r per sifted key of 3d-MDI-QKD (blue, dashed line) and 3d-MDI-QKD with uncharacterized sources (red line). (b) The secret key rate r per sifted key of original MDI-QKD (black, dashed line) and 3d-MDI-QKD (red line). Both secret key rates are obtained under the assumption of uncharacterized sources. The intersection point of the secret key rates appears at the transmission loss 20dB approximately. (c) The secret key rate R per total signal of original MDI-QKD (black, dashed line) and 3d-MDI-QKD (red line) under the assumption of uncharacterized sources. We assume that qubit BSM discriminates two Bell states among four and 3d-BSM does three maximally entangled states among nine. The intersection point appears at transmission loss 10.5dB approximately.

and the phase error rate are both zero within the constraints in Eq. (21) and in Eq. (22). Therefore, in the ideal case, the secret key rate of 3d-MDI-QKD is identical to that of the protocol with uncharacterized sources.

Now, we compare the secret key rate r of original qubit MDI-QKD [51] and 3d-MDI-QKD. In our simulation, r denotes the secret key rate per sifted key. The secret key rate per sifted key of original qubit MDI-QKD is $r_2 = 1 - 2H(Q_b)$, where Q_b is quantum bit error rate (QBER). The secret key rate per sifted key of 3d-MDI-QKD is given in Eq. (4). Fig. 3 (a) shows these two secret key rates. Red line denotes the secret key rate of 3d-MDI-QKD and black dashed line denotes that of original MDI-QKD. As it is seen already [27, 29–31], the secret key rate of 3d-MDI-QKD is higher than that of original MDI-QKD at the same error rate.

The original MDI-QKD has lower secret key rate than BB84 since it has lower sifted key rate. We consider the

sifted key rate in the simulation and show that 3d-MDI-QKD has higher secret key rate than original one even in the realistic experiments. Fig. 3 (b) shows the secret key rate R of original MDI-QKD and 3d-MDI-QKD per total signal. R denotes the secret key rate per total signal. The total signal includes the trials that Alice and Bob can not generate the maximally entangled state and mismatched bases are used in the measurements.

The secret key rate R can be obtained from $R = r \times (\text{sifted key rate})$. The sifted key rate is defined as $(\text{sifted key rate}) = (\text{the probability Alice and Bob choose same basis}) \times (\text{the success probability of BSM})$. Since the original MDI-QKD and 3d-MDI-QKD use two MUBs, the first probability is same with $1/2$. The success probability of BSM is $1/2$ since qubit BSM setup can discriminate two Bell states among four Bell states [56]. There is no proposed 3d-BSM setup with passive linear optical elements yet. In the simulation, we assume that

3d-BSM discriminate three maximally entangled states among nine. In that case, the success probability of 3d-BSM is $1/3$. The secret key rate of original MDI-QKD R_2 is obtained from $R_2 = \frac{1}{4}r_2$ and that of 3d-MDI-QKD is $R_3 = \frac{1}{6}r_3$. In the Fig. 3 (b), the red line denotes R_3 and the black, dashed line shows R_2 . Since the success probability of 3d-BSM is lower than that of qubit BSM, the difference between two key rates is decreased, but still 3d-MDI-QKD always has higher key rate.

Fig. 3 (c) shows the difference between the two key rates $\Delta R = R_3 - R_2$ against ε which is defined in Eq. (16). The factor ε is related with suitability of sources for QKD. The red line and the blue, dashed line denote the case $Q_s = 0.01$ and $Q_s = 0.05$ respectively. ΔR becomes large when ε goes large regardless the state error rate.

Here, we simulate the secret key rate with the change of realistic experimental factors. We consider the two experimental factors, transmission efficiency of photonic channels (η) and dark count rate of single photon detectors (SPDs) d . There is transmission loss when the photon passes through optical fiber or atmosphere, so the transmission efficiency is approximately proportional to the distance which QKD can be achieved. For SPD, since the SPD is very sensitive device, it is possible to be clicked even if no photon enters in SPD. This click produce the dark count in the device. The dark count rate is assumed as 10^{-5} per pulse in the our simulation.

Qubit BSM consists of four SPDs [56] in order to discriminate polarization Bell states of the photons. Contrarily, as it is already mentioned, there is no realistic 3d-BSM setup with passive linear optical elements proposed yet. In our simulation, we assume that 3d-BSM consists of six SPDs to measure two photons and each photon is encoded in three orthonormal states. If there is no Eve, the success probabilities of 3d-BSM is described as

$$p(i, i) = \quad (23)$$

$$\frac{\eta^2(1-d)^4}{3} + 2\eta(1-\eta)d(1-d)^4 + 3(1-\eta)^2d^2(1-d)^4$$

$$p(i, j) = 2\eta(1-\eta)d(1-d)^4 + 3(1-\eta)^2d^2(1-d)^4 \quad (24)$$

where $i, j \in \{0, 1, 2\}$, $i \neq j$ and 3d-BSM discriminates one of the maximally entangled state $|\Phi_0\rangle$ only. In that case, all the probabilities of mismatched basis cases are same, so that $p(i, \bar{j}) = p(j, \bar{i}) = p(\bar{i}, j)$ where $i, j \in \{0, 1, 2\}$. In Eq. (23), the first term describes the situation that two photons trigger off SPDs with $1/3$ success probability. The second term denotes the situation that one photon arrive at SPD and the other photon is lost. In that case, the second SPD is clicked due to the dark count of the detector. The final term denotes the situation that two photons are lost but two SPDs are clicked because of dark counts [57]. With these probabilities, the state error rate and the phase error rate can be calculated and the secret key rates are plotted in Fig. 4 with respect to $(1 - \eta)$.

Fig. 4 (a) shows the secret key rate r of 3d-MDI-QKD (blue, dashed line) and 3d-MDI-QKD with uncharacterized sources (red line) vs. transmission loss. ε is not zero

because of transmission loss in Eq. (24). Since non-zero value of ε is considered as imperfection of communication sources in the security analysis under the assumption of uncharacterized source, 3d-MDI-QKD with uncharacterized sources has lower the secret key rate than 3d-MDI-QKD even if communication sources generate the exact states.

The secret key rate r of original MDI-QKD (black, dashed line) and 3d-MDI-QKD (red line) are shown in Fig. 4 (b). Both secret key rates are calculated under the assumption of uncharacterized sources [57]. 3d-MDI-QKD has higher secret key rate than original MDI-QKD only when transmission loss is low. This effect comes from increased dark counts since 3d-BSM has more SPDs than qubit BSM. The cross point appears at the transmission loss 20dB approximately.

Fig. 4 (c) shows the secret key rate R of original MDI-QKD (black, dashed line) and 3d-MDI-QKD (red line). These secret key rates are calculated from the multiplication between sifted key rate and the secret key rates plotted r shown in Fig. 4 (b). Because of low success probability of 3d-BSM, the difference between two key rates is decreased. The cross point appears at the transmission loss 10.5dB approximately.

V. CONCLUSION

In this paper, we investigated security of 3d-MDI-QKD and that of 3d-MDI-QKD with uncharacterized sources. We assumed that 3d-BSM is able to discriminate three maximally entangled states among nine in the simulation. We showed that 3d-MDI-QKD has higher secret key rate than original qubit MDI-QKD at the same error rate even if we consider sifted key rate. The endurance of 3d-MDI-QKD against low accuracy of the communication sources is better than that of original MDI-QKD as shown in Fig. 3 (c). In the simulation with the realistic experimental parameters, 3d-MDI-QKD has higher key rates only when the transmission loss is low. Since the transmission loss proportional to length of optical fiber, this shows that 3d-MDI-QKD has higher secret key rate only when it is implemented for the short distance communication.

VI. ACKNOWLEDGEMENT

This work was done with support of ICT R&D program of MSIP/IITP (No.2014-044-014-002), National Research Foundation(NRF) grant (No.NRF-2013R1A1A2010537), and National Research Council of Science and Technology(NST) grant (No. CAP-15-08-KRISS).

Appendix A: Calculation of ε in 3d-MDI-QKD with uncharacterized sources

In appendix, we show the details of calculation to obtain Eq. (19). The upper bound of phase error rate is

$$Q_p \leq \langle \tilde{\Phi}_1 | \hat{\rho} | \tilde{\Phi}_1 \rangle + \langle \tilde{\Phi}_2 | \hat{\rho} | \tilde{\Phi}_2 \rangle + Q_s \quad (\text{A.1})$$

from Eq. (14). The first two terms can be calculated from density operator of Alice and Bob

$$\begin{aligned} \langle \tilde{\Phi}_1 | \hat{\rho} | \tilde{\Phi}_1 \rangle &= \frac{1}{3} \frac{\sum_n |\sum_{k=0}^2 \sqrt{p(k, k)} \omega^k e^{i(\delta_k + \xi_k)} \gamma_{kk}(n)|^2}{\sum_{x,y=0}^2 p(x, y)}, \\ \langle \tilde{\Phi}_2 | \hat{\rho} | \tilde{\Phi}_2 \rangle &= \frac{1}{3} \frac{\sum_n |\sum_{k=0}^2 \sqrt{p(k, k)} \omega^{2k} e^{i(\delta_k + \xi_k)} \gamma_{kk}(n)|^2}{\sum_{x,y=0}^2 p(x, y)}, \end{aligned}$$

where $\delta_0 = \xi_0 = 0$. Since Alice and Bob can not determine the exact phases δ and ξ , they should consider the maximum values of these two equation in order to cover

all the possible phase factors. Then the upper bound of the phase error rate becomes

$$Q_p \leq \frac{2}{3} \frac{\sum_n |\sum_{k=0}^2 \sqrt{p(k, k)} e^{i\zeta_k} \gamma_{kk}(n)|^2}{\sum_{x,y=0}^2 p(x, y)} + Q_s.$$

where ζ is the phase which makes maximum the first term. There are γ and ζ factors which Alice and Bob can not determine. Alice and Bob need the upper bound of the phase error rate which is described with the success probabilities of 3d-BSM only. The phase error rate in the ordinary basis must be related with probabilities in bar basis. Therefore, we consider the case that Alice and Bob sends $|\bar{\alpha}_x\rangle$ and $|\bar{\beta}_y\rangle$ to Charlie respectively. After post-selection of successful 3d-BSM case ($|1\rangle_Z$), Eq. (10) becomes

$$\begin{aligned} \hat{U}_E |\bar{\alpha}_x\rangle_C |\bar{\beta}_y\rangle_D |e\rangle_{Ea} &= \sqrt{p(\bar{x}, \bar{y})} |\Gamma \bar{x} \bar{y}\rangle_E \\ &= \sqrt{p(\bar{x}, \bar{y})} \sum_n \gamma_{\bar{x} \bar{y}}(n) |n\rangle_E. \end{aligned} \quad (\text{A.2})$$

The left-hand-side of Eq. (A.2) is described in the ordinary basis from the relations between two bases (Eq. (6)),

$$\begin{aligned} \hat{U}_E |\bar{\alpha}_x\rangle_C |\bar{\beta}_y\rangle_D |e\rangle_{Ea} &= \hat{U}_E \sum_{i,j=0}^2 A_{xi} B_{yj} e^{i(\theta_{xi} + \varphi_{yj})} |\alpha_i\rangle_C |\beta_j\rangle_D |e\rangle_{Ea} \\ &= \sum_{i,j=0}^2 A_{xi} B_{yj} \sqrt{p(i, j)} e^{i(\theta_{xi} + \varphi_{yj})} |\Gamma ij\rangle_E \\ &= \sum_n \sum_{i,j=0}^2 A_{xi} B_{yj} \sqrt{p(i, j)} e^{i(\theta_{xi} + \varphi_{yj})} \gamma_{ij}(n) |n\rangle_E. \end{aligned}$$

With this equation, Eq. (A.2) becomes

$$\sum_n \sum_{i,j=0}^2 A_{xi} B_{yj} \sqrt{p(i, j)} e^{i(\theta_{xi} + \varphi_{yj})} \gamma_{ij}(n) |n\rangle_E = \sqrt{p(\bar{x}, \bar{y})} \sum_n \gamma_{\bar{x} \bar{y}}(n) |n\rangle_E. \quad (\text{A.3})$$

We rearrange the equation to obtain the upper bound of the phase error rate,

$$\begin{aligned} &\sum_n \sum_{i=0}^2 A_{xi} B_{yi} \sqrt{p(i, i)} e^{i(\theta_{xi} + \varphi_{yi})} \gamma_{ii}(n) |n\rangle_E \\ &= \sum_n \left[\sqrt{p(\bar{x}, \bar{y})} \gamma_{\bar{x} \bar{y}}(n) - \sum_{i \neq j}^2 A_{xi} B_{yj} \sqrt{p(i, j)} e^{i(\theta_{xi} + \varphi_{yj})} \gamma_{ij}(n) \right] |n\rangle_E. \end{aligned} \quad (\text{A.4})$$

Doing absolute square on both sides,

$$\begin{aligned} \sum_n \left| \sum_{i=0}^2 A_{xi} B_{yi} \sqrt{p(i, i)} e^{i(\theta_{xi} + \varphi_{yi})} \gamma_{ii}(n) \right|^2 &= p(\bar{x}, \bar{y}) + \sum_n \left| \sum_{i \neq j}^2 A_{xi} B_{yj} \sqrt{p(i, j)} e^{i(\theta_{xi} + \varphi_{yj})} \gamma_{ij}(n) \right|^2 \\ &\quad - \sum_n \sqrt{p(\bar{x}, \bar{y})} \gamma_{\bar{x} \bar{y}}^*(n) \sum_{i \neq j}^2 A_{xi} B_{yj} \sqrt{p(i, j)} e^{i(\theta_{xi} + \varphi_{yj})} \gamma_{ij}(n) \\ &\quad - \sum_n \sqrt{p(\bar{x}, \bar{y})} \gamma_{\bar{x} \bar{y}}(n) \sum_{i \neq j}^2 A_{xi} B_{yj} \sqrt{p(i, j)} e^{-i(\theta_{xi} + \varphi_{yj})} \gamma_{ij}^*(n), \end{aligned} \quad (\text{A.5})$$

since $\sum_n |\gamma_{xy}(n)|^2 = 1$. Considering the phase which makes right-hand-side maximum,

$$\sum_n \left| \sum_{i=0}^2 A_{xi} B_{yi} \sqrt{p(i, i)} e^{i(\theta_{xi} + \varphi_{yi})} \gamma_{ii}(n) \right|^2 \leq \left[\sqrt{p(\bar{x}, \bar{y})} + \sum_{i \neq j}^2 A_{xi} B_{yj} \sqrt{p(i, j)} \right]^2. \quad (\text{A.6})$$

The inequality is satisfied for all phase θ and φ , so

$$\sum_n \left| \sum_{i=0}^2 A_{xi} B_{yi} \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right|^2 \leq \left[\sqrt{p(\bar{x}, \bar{y})} + \sum_{i \neq j}^2 A_{xi} B_{yj} \sqrt{p(i, j)} \right]^2 \quad (\text{A.7})$$

is also satisfied, where ζ is the phase makes left-hand-side maximum. By using triangular inequality, the left-hand-side of the inequality becomes

$$\begin{aligned} & \sum_n \left| \sum_{i=0}^2 A_{xi} B_{yi} \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right|^2 \\ & \geq \sum_n \left[A_{xm} B_{ym} \left| \sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right| - \sum_{i=0}^2 |A_{xm} B_{ym} - A_{xi} B_{yi}| \sqrt{p(i, i)} |e^{i\zeta_i} \gamma_{ii}(n)| \right]^2 \\ & = \sum_n \left[A_{xm}^2 B_{ym}^2 \left| \sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right|^2 + \sum_{i=0}^2 |A_{xm} B_{ym} - A_{xi} B_{yi}|^2 p(i, i) |e^{i\zeta_i} \gamma_{ii}(n)|^2 \right. \\ & \quad \left. - 2 A_{xm} B_{ym} \left| \sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right| \sum_{k=1}^2 D_{xym}(k) |e^{i\zeta_{m+k}} \gamma_{(m+k)(m+k)}(n)| + 2 \prod_{k=1}^2 D_{xym}(k) |e^{i\zeta_{m+k}} \gamma_{(m+k)(m+k)}(n)| \right] \end{aligned} \quad (\text{A.8})$$

where we omit (mod 3) in subscription, $m \in \{0, 1, 2\}$, and $D_{xym}(k)$ is the expression defined as

$$D_{xym}(k) = |A_{xm} B_{ym} - A_{x(m+k)} B_{y(m+k)}| \sqrt{p(m+k, m+k)}.$$

With the help of Cauchy-Schwarz inequality, lower bound of right-hand-side of Eq. (A.8) is obtained.

$$\begin{aligned} & \sum_n \left[A_{xm}^2 B_{ym}^2 \left| \sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right|^2 + \sum_{i=0}^2 |A_{xm} B_{ym} - A_{xi} B_{yi}|^2 p(i, i) |e^{i\zeta_i} \gamma_{ii}(n)|^2 \right. \\ & \quad \left. - 2 A_{xm} B_{ym} \left| \sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right| \sum_{k=1}^2 D_{xym}(k) |e^{i\zeta_{m+k}} \gamma_{(m+k)(m+k)}(n)| + 2 \prod_{k=1}^2 D_{xym}(k) |e^{i\zeta_{m+k}} \gamma_{(m+k)(m+k)}(n)| \right] \\ & \geq \sum_n A_{xm}^2 B_{ym}^2 \left| \sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right|^2 + \sum_{i=0}^2 |A_{xm} B_{ym} - A_{xi} B_{yi}|^2 p(i, i) \sum_n |e^{i\zeta_i} \gamma_{ii}(n)|^2 \\ & \quad - 2 A_{xm} B_{ym} \sum_{k=1}^2 D_{xym}(k) \sqrt{\sum_n \left| \sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right|^2 \sum_{n'} |e^{i\zeta_{m+k}} \gamma_{(m+k)(m+k)}(n')|^2} \\ & = \left[A_{xm} B_{ym} \sqrt{\sum_n \left| \sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right|^2} - \sum_{k=1}^2 D_{xym}(k) \right]^2 - 2 \prod_{k=1}^2 D_{xym}(k) \end{aligned} \quad (\text{A.9})$$

because $\sum_{n=0} |\gamma_{xy}(n)|^2 = 1$. From Eq. (A.7), Eq. (A.8) and Eq. (A.9), we obtain the inequality

$$\left[\sqrt{p(\bar{x}, \bar{y})} + \sum_{i \neq j}^2 A_{xi} B_{yj} \sqrt{p(i, j)} \right]^2 \geq \left[A_{xm} B_{ym} \sqrt{\sum_n \left| \sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right|^2} - \sum_{k=1}^2 D_{xym}(k) \right]^2 - 2 \prod_{k=1}^2 D_{xym}(k) \quad (\text{A.10})$$

Rearranging Eq. (A.10) about $\sum_n |\sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n)|^2$, the inequality becomes

$$\sum_n \left| \sum_{i=0}^2 \sqrt{p(i, i)} e^{i\zeta_i} \gamma_{ii}(n) \right|^2 \leq \frac{1}{A_{xm}^2 B_{ym}^2} \left\{ \sqrt{\left[\sqrt{p(\bar{x}, \bar{y})} + \sum_{i \neq j} A_{xi} B_{yi} \sqrt{p(i, j)} \right]^2} + 2 \prod_{k=1}^2 D_{xym}(k) + \sum_{k=1}^2 D_{xym}(k) \right\}^2 \quad (\text{A.11})$$

only when $A_{xm} B_{ym} \neq 0$. In order to simplify the description, the function S is defined as

$$S_{xy}(m) = \frac{2}{3A_{xm}^2 B_{ym}^2 \sum_{i,j=0}^2 p(i, j)} \left\{ \sqrt{\left[\sqrt{p(\bar{x}, \bar{y})} + \sum_{i \neq j} A_{xi} B_{yj} \sqrt{p(i, j)} \right]^2} + 2 \prod_{k=1}^2 D_{xym}(k) + \sum_{k=1}^2 D_{xym}(k) \right\}^2. \quad (\text{A.12})$$

The upper bound function f and the factor ε is defined with the function S as explained in main text.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984) p. 175.
 - [2] Artur Ekert, Phys. Rev. Lett. **67**, 661 (1991)
 - [3] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
 - [4] D. Mayers, J. Assoc. Comput. Mach. **48**, 351 (2001).
 - [5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
 - [6] I. Devetak, and A. Winter, Proc. R. Soc. Lond. A **461**, 207 (2005).
 - [7] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
 - [8] A. Muller, J. Breguet and N. Gisin, J. Mod. Opt. **41**, 2405 (1994).
 - [9] A. Muller, H. Zbinden, and N. Gisin, Nature **378**, 449 (1995).
 - [10] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
 - [11] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000).
 - [12] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
 - [13] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Nat. Phys. **3**, 481 (2007).
 - [14] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
 - [15] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).
 - [16] W. Son, J. Lee, and M. Kim, J. Phys. A: Math. Gen. **37**, 11897 (2004).
 - [17] P. Rungta, W. Munro, K. Nemoto, P. Deuar, G. Milburn, and C. Caves, Directions in Quantum Optics, Lecture Notes in Physics **561** 149 (2001).
 - [18] S. L. Braunstein, G. M. D'Ariano, G. J. Milburn, and M. F. Sacchi, Phys. Rev. Lett. **84**, 3486 (2000).
 - [19] W. Son, J. Lee, M. S. Kim, and Y. J. Park, Phys. Rev. A **64**, 064304 (2001).
 - [20] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **93**, 010503 (2004).
 - [21] I. A. Khan and J. C. Howell, Phys. Rev. A **73**, 031801 (2006).
 - [22] L. Neves, G. Lima, J. G. AouirGomez, C. H. Monken, C. Saavedra, and S. Pádua, Phys. Rev. Lett. **94**, 100501 (2005).
 - [23] M. N. O'Sullivan-Hale, I. A. Khan, R. W. Boyd, and J. C. Howell, Phys. Rev. Lett. **94**, 220501 (2005).
 - [24] C. Schaeff, R. Polster, R. Lapkiewicz, R. Fickler, S. Ramelow, and A. Zeilinger, Optics Express **20**, 16145 (2012).
 - [25] J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial, Phys. Rev. Lett. **88**, 257901 (2002).
 - [26] M. Malik, M. Erhard, M. Huber, M. Krenn, R. Fickler, and A. Zeilinger, Nat. Photonics **10**, 248 (2016).
 - [27] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
 - [28] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. Cerf, J. Phys. A: Math. Gen. **35**, 10065 (2002).
 - [29] T. Durt, D. Kaszlikowski, J. L. Chen, and L. C. Kwek, Phys. Rev. A **69**, 032313 (2004).
 - [30] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).
 - [31] A. Ferenczi and N. Lütkenhaus, Phys. Rev. A **85**, 052310 (2012).
 - [32] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Nat. Commun. **7**, 11712 (2016).
 - [33] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A, **61**, 062308 (2000).
 - [34] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. **98**, 060503 (2007).
 - [35] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, Phys. Rev. A **87**, 062322 (2013).

- [36] J. Nunn, L. Wright, C. Söller, L. Zhang, I. Walmsley, and B. Smith, *Optics Express* **21**, 15959 (2013).
- [37] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. SoutoRibeiro, *Phys. Rev. Lett.* **96**, 090501 (2006).
- [38] S. Etcheverry, G. Cañas, E. Gómez, W. Nogueira, C. Saavedra, G. Xabier, and G. Lima, *Sci. Rep.* **3**, 2316 (2013).
- [39] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, *N. J. Phys.* **8**, 75 (2006).
- [40] M. Mirhosseini, O. Magaña-Loaiza, M. O’Sullivan, B. Rodenburg, M. Malik, M. Lavery, M. Padgett, D. Gauthier, and R. Boyd, *N. J. Phys.* **17**, 033033 (2015).
- [41] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Phys. Rev. Lett.* **85**, 1330 (2000).
- [42] V. Makarov and D. Hjelme, *J. Mod. Opt.* **52**, 691 (2005).
- [43] V. Makarov, A. Anisimov, and J. Skaar, *Phys. Rev. A* **74**, 022313 (2006).
- [44] mode.) L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Nat. Photonics* **4**, 686 (2010).
- [45] B. Qi, C. Fung, H. Lo, and X. Ma, *Quantum Inf. Comput.* **7**, 73 (2007).
- [46] A. N. Bugge, S. Sauge, AinaMardhiyahM. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, *Phys. Rev. Lett.* **112**, 070503 (2014).
- [47] W. Hwang, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [48] A. Acín, N. Gisin, and L. Masanes, *Phys. Rev. Lett.* **97**, 120405 (2006).
- [49] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007).
- [50] J. Clauser, M. Horne, A. Shimony, and R. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).
- [51] H. K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [52] H. Lo, M. Curty, and K. Tamaki, *Nat. Photonics* **8**, 595 (2014).
- [53] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, *Phys. Rev. Lett.* **111**, 130501 (2013).
- [54] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H. K. Lo, *Phys. Rev. Lett.* **112**, 190503 (2014).
- [55] Y. L. Tang, H. L. Yin, S. J. Chen, Y. Liu, W. J. Zhang, X. Jiang, L. Zhang, J. Wang, L. X. You, J. Y. Guan, D. X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T. Y. Chen, Q. Zhang, and J. W. Pen, *Phys. Rev. Lett.* **113** 190501 (2014).
- [56] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, *Phys. Rev. A* **59**, 3295 (1999).
- [57] Z. Q. Yin, Chi-HangFred Fung, X. Ma, C. M. Zhang, H. W. Li, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, *Phys. Rev. A* **90**, 052319 (2014).
- [58] W. Wootters and B. Fields, *Annals of Physics* **191**, 363-381 (1989).
- [59] V. Coffman, J. Kundu, and W. K. Wootters, *Phys. Rev. A* **61**, 052306 (2000).
- [60] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, *Phys. Rev. Lett.* **71**, 4287 (1993).